НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ПРОГРАМА ФАХОВОГО ВСТУПНОГО ІСПИТУ «УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для вступників на навчання для здобуття ступеня магістра за спеціальністю К3 «Національна безпека» (за окремими сферами забезпечення і видами діяльності), освітня програма – кіберзахист у сфері інформаційних технологій та кіберпросторі

Київ-2025

1. Загальні положення

Національна академія Служби безпеки України (далі – Академія) згідно з Порядком прийому на навчання для здобувачів вищої освіти в 2025 році, затвердженого наказом Міністерства освіти і науки України від 10 лютого 2025 року № 168, зареєстрованого у Міністерстві юстиції України 26 лютого 2025 року за № 15/41360, та Правилами прийому до Національної академії Служби безпеки України у 2025 році, проводить фаховий вступний іспит «Управління інформаційної безпеки» для конкурсного відбору вступників на навчання для здобуття другого (магістерського) рівня вищої освіти денної та заочної форми навчання за спеціальністю К3 «Національна безпека» (за окремими сферами забезпечення і видами діяльності) освітньо-професійна програма «Кіберзахист у сфері інформаційних технологій та кіберпросторі».

Ця Програма розроблена фаховою атестаційною комісією з управління інформаційної безпеки Приймальної комісії Академії.

2.Вимоги до компетентності вступників з управління інформаційної безпеки

Вимоги до компетентності вступників з управління інформаційної безпеки визначено з урахуванням положень законодавства України у сфері захисту інформації та цілей і змісту навчання за освітньо-професійними програмами підготовки фахівців для професійної діяльності за спеціальністю К3 «Національна безпека» (за окремими сферами забезпечення і видами діяльності).

Відповідність рівня компетентності вступника визначається шляхом перевірки рівня володіння знаннями у сфері захисту інформації та уміннями застосовувати їх для вирішення завдань кіберзахисту у сфері інформаційних технологій та кіберпросторі.

Навчальний матеріал, що виноситься на фахове вступне випробування, структурований за такими змістовними модулями:

- окремі тематичні положення нормативно-правового забезпечення у сфері інформаційної безпеки та кібербезпеки;
- основи інформаційних технологій;
- мови і технології програмування;
- комп’ютерні системи та мережі;
- кіберзахист інформаційних ресурсів.

2.1. Окремі тематичні положення нормативно-правового забезпечення у сфері інформаційної безпеки та кібербезпеки

Закон України «Про інформацію». Закон України «Про національну безпеку України». Закон України «Про основні засади забезпечення кібербезпеки України». Закон України «Про Державну службу спеціального зв’язку та захисту інформації». Закон України «Про державну таємницю». Закон України «Про захист інформації в інформаційно-комунікаційних системах». Закон України «Про Національну програму інформатизації».

Закон України «Про Раду національної безпеки і оборони України». Указ Президента України від 16 лютого 2022 року № 56/2022 «Про Стратегію забезпечення державної безпеки». Указ Президента України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». Указ Президента України від 26 серпня 2021 року «Про Стратегію кібербезпеки України».

2.2. Основи інформаційних технологій

Інформація. Властивості інформації. Кількісні характеристики інформації. Види інформації та їх класифікація. Вимірювання інформації. Процеси перетворення та кодування інформації.

Поняття про системи числення. Принципи, методи і форми збереження інформації в пам’яті ПЕОМ. Принципи обробки даних на ПЕОМ. Представлення даних. Системи числення. Формати даних.

Структура персонального комп’ютера. Класифікація ПК. Види корпусів. Блоки живлення. Материнська плата. Центральний процесор. Оперативна пам’ять. Плати адаптерів. Пристрої зберігання даних. Пристрої введення/виведення даних. Класифікація та налаштування принтерів. Способи покращення роботи апаратного забезпечення.

Інформаційні технології у різних сферах життєдіяльності. Види інформаційних технологій. Інформаційні системи. Базові інформаційні процеси. Технології розподіленої обробки даних. Класифікація інформаційних систем. Математичне та програмне забезпечення інформаційних систем.

Мультимедійні технології. Геоінформаційні технології. Інформаційні технології зв'язку. Інтелектуальні інформаційні технології.

2.3. Мови і технології програмування

Мови програмування. Структурне програмування. Об’єктно-орієнтоване програмування. Роль алгоритмів у програмуванні. Внутрішня організація комп’ютера. Архітектура фон Неймана. Життєвий цикл програмного забезпечення. Методології розробки програмного забезпечення. Компілятори. Алгоритмізація задач. Властивості алгоритмів, їх класифікація. Схеми алгоритмів. Лінійні, розгалужені, циклічні та комбіновані алгоритми.

Ідентифікатори. Змінні та константи. Типи даних. Організація введення-виведення даних. Арифметичні операції. Пріоритет виконання операцій.

Оператор розгалуження if. Логічні вирази. Оператор вибору switch. Операції інкремента та декремента. Цикли з лічильником for, цикли з перед умовою та після умовою.

Пошук у одновимірних та багатовимірних масивах. Поняття підпрограми. Основні принципи побудови функцій. Оголошення функцій, опис та виклик функцій. Формальні та фактичні параметри.

Символьні рядки та функції над рядками. Структури. Доступ до елементів структури. Масиви структур. Вказівники на структури.

Класи. Інкапсуляція. Поліморфізм. Успадкування.

Функції зчитування та запису інформації у файли, функції пошуку у файлах.

2.4. Комп’ютерні системи та мережі

Технології передачі даних у мережах. Рівні моделі OSI. Характеристика стандартів IEEE 802.xx. Топології комп’ютерних мереж. Хости. Протоколи.

Апаратне і програмне забезпечення комп'ютерних мереж. Пристрої та обладнання локальних мереж (повторювач, міст, концентратори). Комутатори (MAC-адреси, моніторинг, фільтрація, функції безпеки, прив'язка портів). Маршрутизатори та шлюзи. Точка доступу. Протоколи та засоби керування в комп’ютерних мережах.

Програмне забезпечення комп’ютерних мереж. Стек протоколів TCP/IP як основа мережі Інтернет TCP/IP. Мережевий рівень в Інтернет. Система IP-адресації. Технології розподілу мережного простору. Транспортна служба. Типи мережевих з'єднань. Логічна модель транспортного рівня.

Середовища передавання сигналів. Носії передавання інформації (вита пара, коаксіальний кабель, оптоволокно). Безпровідний зв’язок. Електромагнітний спектр, радіозв’язок, зв’язок у мікрохвильовому діапазоні, інфрачервоні і міліметрові хвилі, зв’язок у видимому діапазоні, супутниковий зв’язок, мобільний телефонний зв’язок, кабельне телебачення. Характеристика носіїв передачі інформації.

2.5 Кіберзахист інформаційних ресурсів

Інтернет-безпека, кібербезпека та захист інформації в комп’ютерних мережах. Сегментація мереж. Маршрутизація у глобальній мережі Інтернет. Безпека комп’ютерних мереж. Проблеми і категорії безпеки мереж. Методи несанкціонованого доступу до інформації та мереж. Захист від атак. Криптографічні засоби захисту. Основні засоби та стратегії захисту комп'ютерних мереж. Фільтрація пакетів і протоків. Міжмережевий екран.

Адміністрування комп’ютерних мереж. Пристрої віртуальних приватних мереж. Принципи VPN. Програмні VPN. Апаратні VPN. Організація доменної моделі комп’ютерної мережі.

Питання безпеки у мережі Internet. Види атак на систему. Методи протидії. Апаратне забезпечення для організації безпеки мережі. IDS системи. IPS системи. Мережі на основі тонкого клієнта. Характеристики, призначення, функціональні можливості. Організація безпечного доступу до ресурсів локальної мережі. Віртуалізація та хмарні обчислення.

Інтернет речей. Основні відомості. Еталонна модель IoT. Приклади застосування та організація взаємодії. Спрощена структура IoT.

3. Специфікація фахового вступного іспиту «Управління інформаційної безпеки»

3.1. Академія проводить фаховий вступний іспит «Управління інформаційної безпеки» у письмовій формі із використанням технологій тестування.

Кожному вступникові надається екзаменаційний білет, що містить п’ять тестових питань, які передбачають вибір правильної відповіді із декількох

запропонованих на кожне питання, а також одне питання для самостійного письмового викладу його змісту. Питання надаються відповідно до обсягу навчального матеріалу, визначеного в пункті 2 цієї Програми. Зміст відповіді вступник фіксує на виданих йому аркушах встановленого зразка, які після закінчення випробування передає секретарю комісії.

3.2. Результати фахового випробування оцінюються за 200-бальною шкалою шляхом додавання балів за результатами відповідей на тестові запитання (по 20 балів за кожну правильну відповідь) та оцінки комісією рівня відповіді на питання для самостійного письмового викладу за шкалою від 1 до 100 балів. Мінімальний бал із фахового іспиту «Управління інформаційної безпеки», з яким вступник допускається до подальшої участі в конкурсному відборі для зарахування на навчання, складає 100 (сто) балів.

Відповіді вступників на кожне із питань екзаменаційного білету оцінюються комісією на підставі таких критеріїв:

Бали	**Критерії оцінювання**
1-10	Вступник може на рівні «так-ні» відтворити кілька термінів з обсягу питання, обрати правильний варіант відповіді з двох запропонованих.
11-20	Вступник може двома-трьома простими реченнями передати основний зміст питання, має про нього загальне уявлення.
21-30	Вступник може, відтворити більшу частину основного змісту питання, дати визначення поняття.
31-40	Вступник може: відтворити основний зміст питання, визначити поняття й охарактеризувати його окремі ознаки
41-50	Вступник може: самостійно викласти матеріал основного змісту питання, застосовуючи необхідну термінологію; дати визначення понять; підтвердити одним, двома аргументами висловлене ним оцінювальне судження.
51-60	Вступник володіє матеріалом змісту питання і використовує знання за аналогією, може порівнювати, узагальнювати, систематизувати інформацію.
61-70	Вступник вільно оперує матеріалом змісту питання, узагальнює та аналізує окремі визначення та принципи, формулює висновки та обґрунтовує їх конкретними аргументами.
71-80	Вступник вільно викладає зміст питання, застосовуючи необхідну термінологію та нормативно-правову базу, робить аргументовані висновки.
81-90	Вступник може вільно викладати власні судження й переконливо їх аргументувати, самостійно аналізує положення чинного законодавства, які стосуються питання.
91-100	Вступник володіє глибокими й міцними знаннями, дає ґрунтовну відповідь на поставлене питання, викладає власну позицію і переконливо її аргументує, критично оцінює зміст нормативних актів, що стосуються питання, вміє узагальнити поданий матеріал.

3.3.Оцінка відповіді вступника проводиться згідно із зазначеними у п. 3.2 цієї Програми критеріями оцінювання не менше ніж двома членами комісії, які виносять результати оцінки відповіді на загальне обговорення. Оцінки за результатами фахового вступного іспиту виставляються за результатами їх загального обговорення на засіданні фахової атестаційної комісії.

Результати фахового вступного іспиту фіксуються у відомості складання фахового вступного іспиту та оголошуються вступникам не пізніше наступного дня після проведення фахового вступного іспиту.

3.4. Вступникам під час фахового вступного іспиту забороняється користуватись електронними засобами, підручниками, навчальними посібниками та іншими матеріалами, якщо це не передбачено рішенням Приймальної комісії.

У разі використання вступником під час фахового вступного іспиту сторонніх джерел інформації, він відсторонюється від подальшого складання іспиту та участі в конкурсному відборі, про що складається акт.

Перескладання фахового вступного іспиту не дозволяється.

Апеляції на результати іспиту розглядає апеляційна комісія Академії у порядку, визначеному Правилами прийому.

4. Акти законодавства України, що зазначені в Програмі

Акти законодавства України, що зазначені в Програмі слід вивчати за їх текстами в останній редакції, що міститься у Відомостях Верховної Ради України, Офіційному віснику України, інших офіційних виданнях України, а також на сайті Верховної Ради України (www.rada.gov.ua).

Додаток

ПЕРЕЛІК ПИТАНЬ
ФАХОВОГО ВСТУПНОГО ІСПИТУ
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для вступників на навчання для здобуття ступеня магістра
за спеціальністю К3 «Національна безпека» (за окремими сферами забезпечення і видами діяльності), освітня програма – кіберзахист у сфері інформаційних технологій та кіберпросторі

Київ – 2025

Окремі тематичні положення нормативно-правового забезпечення у сфері інформаційної безпеки та кібербезпеки

1. Види інформації за змістом відповідно до Закону України «Про інформацію».
2. Порівняти поняття «кіберзагрози», «кіберзлочину» та «кібертероризму» відповідно до Закону України «Про основні засади забезпечення кібербезпеки України».
3. Правові основи забезпечення кібербезпеки України.
4. Національна система кібербезпеки.
5. Об’єкти критичної інфраструктури.
6. Основні завдання Державної служби спеціального зв’язку та захисту інформації України.
7. Описати умови обробки інформації в системі відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах».
8. Національна програма інформатизації відповідно до Закону України «Про Національну програму інформатизації»
9. Описати функції Ради національної безпеки і оборони України
10. Поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов
11. Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки
12. Пріоритети національних інтересів України та забезпечення національної безпеки

Основи інформаційних технологій

1. Поняття інформації, співвідношення понять «інформація» і «дані».
2. Властивості інформації.
3. Класифікація та призначення інформаційних технологій.
4. Застосування інформаційних технологій у сфері національної безпеки
5. Інформаційні технології та соціальні мережі
6. Пошукові системи
7. Інформаційні технології та кібербезпека
8. Інформаційні ресурси та форми їх існування.
9. Етапи перетворення інформації
10. Процес передавання інформації та роль кодування інформації в ньому
11. Вимірювання інформації
12. Кодування даних різного типу.
13. Логічна структура персонального комп’ютера.
14. Материнська плата, характеристики та класифікація материнських плат.
15. Процесор. Види процесорів.
16. Оперативна пам’ять. Види оперативної пам’яті.
17. Жорсткий диск. Класифікація жорстких дисків.

18. BIOS та особливості його налаштування.
19. Пристрої зберігання даних.
20. 3D-принтери та їх характеристики.
21. Використання VR-гарнітури та AR-гарнітури.
22. RAID-масиви

Мови і технології програмування

1. Ідея об’єктно-орієнтованого програмування.
2. Архітектура фон Неймана.
3. Лінійні, розгалужені, циклічні та комбіновані алгоритми
4. Методології розробки програмного забезпечення.
5. Організація введення-виведення даних на одній із мов програмування.
6. Масиви. Класифікація масивів.
7. Оператор розгалуження if. Форми запису оператору розгалуження.
8. Основні принципи побудови функцій.
9. Класифікація мов програмування.
10. Формальні та фактичні параметри функцій користувача
10. Структури у програмуванні. Масиви структур.
11. Вказівники та їх роль у програмуванні.
12. Функції зчитування та запису інформації у файли, функції пошуку у файлах.

Комп’ютерні системи та мережі

1. Характеристики комп'ютерної мережі типу LAN
2. Характеристики комп'ютерної мережі типу VLAN
3. Особливості організації та налаштування мережі типу VPN
4. Характеристики мереж із дротовим з’єднанням.
5. Характеристики мереж стільникового зв’язку.
6. Характеристики супутникового зв’язку.
7. Мережеві карти та їх види.
8. Класифікація видів мережевого обладнання.
9. Різниця між коаксіальними та оптоволоконними кабелями.
10. Види віртуалізації.
11. Класифікація сервісів для здійснення хмарних обчислень.
12. Рівні моделі OSI

Кіберзахист інформаційних ресурсів

1. Класифікація зловмисного програмного забезпечення.
2. Основні типи зловмисних атак.
3. Основні засоби організації безпеки ПК та мереж.
4. Політики безпеки.
5. Сегментація мереж.
6. Маршрутизація у глобальній мережі Інтернет.
7. Безпека комп’ютерних мереж.
8. Класифікація міжмережевих екранів.

9. Апаратне забезпечення для організації безпеки мережі.
10. IDS системи
11. IPS системи
12. Організація безпечного доступу до ресурсів локальної мережі.